

BITCOINS
VERWAHREN
UND
VERERBEN

EIN PRAKTISCHER RATGEBER

MARC
STEINER

APRYCÖT

BITCOINS
VERWAHREN
UND
VERERBEN

EIN PRAKTISCHER RATGEBER

MARC
STEINER

APRYCÖT

DER ERSTE AUTOR, DER DEN BITCOIN- NACHLASS VERSTÄNDLICH ERKLÄRT!

In seinem praktischen Ratgeber zeigt Digitalexperte und Bitcoinberater Marc Steiner simpel und auf den Punkt, wie du deine Bitcoins sicher verwahrst und vererbst. Ob Einsteiger oder Fortgeschrittene: Anschaulich führt er dich zu einem verlässlichen, auf deine individuellen Bedürfnisse zugeschnittenen Nachlassplan. So hast du die Zukunft deiner Bitcoins jederzeit selbst in der Hand.

MIT KOSTENLOSEM HILFSTOOL FÜR DICH UND
KURZANLEITUNG FÜR DEINE ERBEN!

www.marcsteiner.tech

BITCOINS
VERWAHREN
UND
VERERBEN

EIN PRAKTISCHER RATGEBER

MARC
STEINER

Lektorat: Dmitrij Gawrisch

Korrektorat: Tanja Giese

Buchgestaltung: Boris Gassmann & Fabian Widmer

E-Book-Konvertierung: CPI books GmbH, Leck

Verlag: Aprycot Media - Held & Troendle GbR - Muldenweg 8, 79618 Rheinfeldern

www.aprycot.media / Twitter: [@aprycotmedia](https://twitter.com/aprycotmedia)

1. Auflage 2020

ISBN: 978-3-9821095-7-2 (Print)

ISBN: 978-3-9821095-8-9 (ePub)

www.marcsteiner.tech

Copyright © 2020 by Marc Steiner

Copyright © 2020 by Aprycot Media - Held & Troendle GbR

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung ist ohne schriftliche Zustimmung des Urhebers unzulässig. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Haftungsbeschränkung/Ausschluss von Garantien: Obwohl Autor und Verlag bei der Erstellung dieses Buches alle Anstrengungen unternommen haben, geben sie keine Zusicherungen oder Gewährleistungen in Bezug auf die Richtigkeit oder Vollständigkeit des Inhalts dieses Buches und lehnen insbesondere alle stillschweigenden Gewährleistungen der Marktgängigkeit oder Eignung für einen bestimmten Zweck ab. Es kann keine Gewährleistung durch Handelsvertreter oder schriftliche Verkaufsunterlagen geschaffen oder erweitert werden. Die hierin enthaltenen Ratschläge und Strategien eignen sich möglicherweise nicht für Ihre persönliche Situation. Sie sollten sich gegebenenfalls an einen Fachmann wenden. Weder der Verlag noch der Autor haften für entgangene Gewinne oder andere kommerzielle Schäden, einschließlich aber nicht beschränkt auf besondere, zufällige, Folge- oder sonstige Schäden.

Für meine Töchter Ava und Ivy

Inhalt

[Vorwort von Jonas Schnelli](#)

K1 SORGE RECHTZEITIG VOR

[Verliere keine Zeit](#)

[Das erwartet dich](#)

[Für Geeks und Updates](#)

[Mein Hilfstool](#)

K2 DU BRAUCHST EINEN NACHLASSPLAN

[Es lohnt sich immer](#)

[Aus Fehlern gelernt](#)

[Der Nachlassplan, der dir entspricht](#)

[Bereite deine Erben vor](#)

K3 DIE REVOLUTION VON SATOSHI NAKAMOTO

[Satoshis Vermächtnis](#)

[Blockchain](#)

[Full Nodes](#)

[Mining](#)

[Asymmetrische Kryptografie](#)

[Alles ist möglich](#)

K4 WALLETS KENNEN UND VERSTEHEN

[Deine Schlüssel speichern und verwalten](#)

[Das Wallet-Universum](#)

[Automatischer Backup dank Seed-Phrase](#)

[HD-Wallets erklärt](#)

[Wallet-PIN, Wallet-Passwort und Passphrase](#)

Hardware-Wallets

Software-Wallets

«Analoge» Wallets

Papier-Wallets

Brain-Wallets

K5 MACHE DEINE IT SICHER

Verwende aktuelle Software

Erstelle sichere Passwörter

Richte 2-Faktor-Authentifizierung ein

Nutze Offline-Systeme oder Tails OS

Verschlüsse deine Daten

K6 SETZE DEINEN NACHLASSPLAN UM

In drei Schritten zum Ziel

Vertrauenswürdige Personen finden

Informationen festhalten

Ausdrucke und Kopien

Informationen elektronisch speichern

Mein Hilfstool nutzen

Den Nachlassplan sicher verwahren

Metall-Seed-Speicher

Schutz vor Wasser

Schutz vor Feuer

Schutz elektronischer Speichermedien

Sichere Orte bestimmen

Die Erben informieren

Erben selber informieren

Vertrauensperson informiert deine Erben

Erben elektronisch informieren

Testament nutzen

Tools für Fortgeschrittene

[Multisignatur](#)
[Shamir's Secret Sharing Scheme](#)
[Poor Man's Shamir's Secret Sharing Scheme](#)
[Denke einfach, denke langfristig](#)
[Rechtliches beachten](#)

K7 MUSTERABLÄUFE

[#1: Grundvariante](#)
[#2: Zusätzliche Sicherheitshürde](#)
[#3: Volldigital umgesetzt](#)
[#4: Kombination mit einem Testament](#)
[#5: Poor Man's Shamir's Secret Sharing Scheme](#)
[#6: «SLIP-0039» Shamir's Secret Sharing Scheme](#)
[#7: «Digitales» Shamir's Secret Sharing Scheme](#)
[#8: Multisignatur mit Hardware-Wallet](#)
[Empfohlene Hersteller](#)

[Geschafft!](#)

ANLEITUNG FÜR DIE ERBEN

ANHANG

[Antworten auf häufige Fragen \(FAQ\)](#)

[Glossar](#)

[Stichwortverzeichnis](#)

[Quellenverzeichnis](#)

[Über den Autor](#)

Dank

Allein hätte ich dieses Buch niemals schreiben können. Ich möchte meiner Frau Angela für die vielen Ideen und Diskussionen danken und dafür, dass sie mir den Rücken gestärkt und Freiraum zum Schreiben gelassen hat. Claudia Fekete und Dennis Nagpal danke ich für ihre Geduld bei der Überarbeitung der allerersten, noch sehr chaotischen Manuskriptfassung. Mein Vater hat wichtige Fragen gestellt und sich nicht mit halben Antworten zufriedengegeben - vielen Dank dafür sowie für die enorme Mithilfe beim Stichwortverzeichnis. Meine Mutter und Schwester gaben mir wertvolle Inputs und wurden nie müde, mit mir zu diskutieren. Dominik Spicher und Raphael Baumann halfen mir technisch und juristisch weiter. Vielen Dank an Lucas Betschart, «Hoewe», Thomas Lobeck und «Alex» für die anregenden Gespräche. Jonas Schnell danke ich für sein Vorwort, Pascal Hügli für seine wertvollen Hinweise rund ums Schreiben eines Sachbuchs.

Meinem Sparringspartner Dmitrij Gawrisch danke ich für das hervorragende Lektorat, Boris Gassmann und Fabian Widmer für die tolle Gestaltung und Tanja Giese für das Ausbessern auch der kleinsten Fehler. Für ihr Vertrauen und die unkomplizierte Zusammenarbeit danke ich meinen beiden Verlegern von Aprycot Media, Stefan Held und Fabio Troendle. Dafür, dass er den Bitcoin erschaffen hat, danke ich Satoshi Nakamoto. Gewidmet habe ich diesen praktischen Ratgeber rund um die Verwahrung und Vererbung von Bitcoins meinen beiden Töchtern. Ihr seid mitten im Hype um die Kryptowährung geboren. Dank euch habe ich gelernt, früh aufzustehen und die Zeit effizienter zu nutzen, zum Beispiel um an diesem Buch zu schreiben.

Ihr habt mich daran erinnert, mit welcher Freude Kinder Neues ausprobieren und entdecken - und wie sehr es sich lohnt, diese Freude und Leidenschaft auch im Erwachsenenalter beizubehalten. Ich liebe euch über alles, ihr seid meine Inspiration. Euch gehört die Zukunft.

Vorwort von Jonas Schnelli

Wie einst das Internet ist der Bitcoin gerade dabei, die (Finanz-)Welt zu revolutionieren. Mithilfe dieser ersten, ältesten und mit Abstand meistverwendeten Kryptowährung können große Vermögenswerte innerhalb von Minuten übertragen werden - ohne Mittelsmann, zensurresistent, fast gebührenfrei, weltweit. Die kryptografischen Schlüssel, die den Zugriff auf die Bitcoins ermöglichen, können kopiert und an verschiedenen Orten sicher aufbewahrt werden, und wo die Schlüssel sind, da sind immer auch die Bit-coins. Mittels mehrfacher Signaturen lassen sich die Vermögenswerte sogar verteilt sichern, ein kryptografiegestütztes Mehr-Augen-Prinzip. Und das ist noch lange nicht alles. Der Bitcoin bietet bahnbrechende Möglichkeiten der selbständigen Vermögensverwaltung. Nicht umsonst heißt es in der Szene: Nur wer seine Bitcoins selber verwaltet, besitzt Bitcoins.

Doch mit dem Potential steigen bekanntlich auch die Risiken. Wer «seine eigene Bank» betreibt, muss strenge Sicherheitsvorkehrungen treffen - und bisweilen auch seine Denk- und Verhaltensmuster hinterfragen und anpassen. Nicht anders als das beim Einzug des Internets, dieses anderen «Game Changers», der Fall war. Immer wieder verschwinden kleine und große Summen auf Nimmerwiedersehen im Datennirwana, weil Nutzer ihre Passwörter vergessen oder ihre digitalen Schlüssel verlieren. Wer mit Bitcoins handelt, muss lernen, seine Zugangsdaten sicher zu verwahren. Es besteht kein Zweifel: Obwohl der Bitcoin noch ein relativ junges Phänomen ist, ist er gekommen, um zu bleiben. Je

verbreiteter die Kryptowährung wird, je mehr Menschen mit ihr Handel treiben, desto relevanter wird auch die Frage, wie man sein kryptografisches Vermögen sicher an die nächste Generation vererbt. Dieses Buch gibt darauf praxisnahe Antworten. Lesen Sie es! Es wirft ein Licht auf einen Aspekt der neuen Technologie, der viel zu lange unbeachtet im Dunkeln geblieben ist.

Jonas Schnelli ist Bitcoin Core Developer und Maintainer

HODL



KAPITEL



SORGE RECHTZEITIG VOR

Hier erfährst du, warum jeder Mensch, der Bitcoins besitzt, unbedingt einen Nachlassplan für deren Vererbung erstellen sollte. Du lernst, wie dieser praktische Ratgeber aufgebaut ist, wie du ihn benutzt und wo du ergänzende Informationen findest. Zudem stelle ich mein kostenloses Hilfstool vor, das dir bei deiner ganz persönlichen Nachlassplanung noch gute Dienste leisten wird.

Verliere keine Zeit

Vererbung ist ein Thema, das viele Menschen vor allem im jungen Alter allzu gern auf die lange Bank schieben. Ich bin da keine Ausnahme. Wer will sich schließlich schon vorzeitig mit seinem Ende befassen, den denkbaren Folgen eines Autounfalls oder einer schweren Erkrankung wie etwa Demenz ins Auge blicken? Obwohl die Angst absolut verständlich ist, sollte sie dich, lieber Leser, aber nicht davon abhalten, genau das zu tun. Sorge, solange du dich eines klaren Verstandes und bester Gesundheit erfreust, für den Fall der Fälle vor. Vielleicht besitzt du ein Haus oder ein Auto, Aktien oder Gemälde, höchstwahrscheinlich lautet mindestens ein Bankkonto auf deinen Namen. Mit all diesen «analogen» Vermögenswerten bist du vertraut und weißt, wie du sie vererben kannst oder wer dir dabei hilft.

Aber weißt du auch, was mit deinen Bitcoins passiert, wenn es dich eines Tages nicht mehr geben sollte? So viel sei hier bereits verraten: Bei der Kryptowährung ist das ohnehin alles andere als triviale Vererbungsunterfangen noch einmal deutlich komplizierter. Der Bitcoin hat das Geld aus den Fängen des traditionellen zentralistischen Finanzsystems befreit und dich zum alleinigen Herren darüber gemacht. Das ist die gute Nachricht. Die schlechte: Um die Verwahrung und Vererbung dieses Vermögenspostens musst du dich nun ganz allein kümmern, es gibt keine Helpline, die du oder deine Erben anrufen könnten. Die «Null-Fehler-Toleranz», die in der kryptografischen Bitcoinwelt üblich ist, macht die Sache nicht einfacher. Man liest immer wieder von Missgeschicken, die selbst technisch versierten Profis passieren. So kommt es zum Beispiel regelmäßig vor, dass

Nutzer ihre Coins an eine falsche Adresse schicken. Getätigte Transaktionen lassen sich in den seltensten Fällen noch abfangen. Sind sie einmal in der Blockchain bestätigt, ist der Zug in der Regel abgefahren.

Das wäre höchstwahrscheinlich auch der Fall, wenn dir etwas zustoßen sollte, bevor du dich um dein Bitcoinerbe gekümmert hast. Kommt hinzu: Für deine Erben ist der Bitcoin vermutlich Neuland. Deshalb solltest du ihnen nicht nur rechtzeitig die Zugangsdaten zu deinem Kryptogeld übergeben, sondern einen kompletten Nachlassplan, der ihnen Schritt für Schritt erklärt, was sie tun müssen, um an dein Erbe heranzukommen. Dabei ist jederzeit Vorsicht geboten: Lässt du den Nachlassplan oder gar deine Zugangsdaten offen herumliegen, machst du es Angreifern allzu leicht, dein Konto leerräumen. Versteckst du die Zugänge aber so, dass die Erben sie nicht finden, oder regelst deinen Nachlass nicht rechtzeitig, sind deine kostbaren Bitcoins für immer weg. Verliere deshalb keine Zeit und Sorge möglichst bald für den Fall der Fälle vor. Sonst könnte alles, was du zu Lebzeiten erreicht hast, für die Katz gewesen sein.

Mein Buch richtet sich an alle, die Bitcoins bereits besitzen, sie sicher verwahren und eines Tages vererben möchten. Egal ob du Einsteiger bist oder fortgeschrittener Anwender, im Laufe der Lektüre kriegst du praktische Tipps, wie du mit einfachen Mitteln einen auf dich und deine individuellen Bedürfnisse zugeschnittenen Nachlassplan erstellen und sicher verwahren kannst. Du findest kompakte Anleitungen zu möglichen Vererbungsabläufen und lernst, selbst vor unkonventionellen Methoden nicht zurückzuscheuen. Als Inspirationsquelle und Nachschlagewerk in einem soll dir

mein praktischer Ratgeber helfen, an Dinge zu denken, die du selbst vielleicht nicht bedacht hättest.

Besitzt du neben dem Bitcoin noch andere Coins oder Tokens? Auf die Vielfalt der Kryptos gehe ich als überzeugter Bitcoiner nur am Rande ein, deren Vererbung aber läuft nach den gleichen Prinzipien ab, wie ich sie hier beschreibe. Die Aussagen und Instrumente dieses Buches kannst du somit auch auf andere Krypto-Assets anwenden. Die Technologie in diesem Bereich entwickelt sich rasend schnell. Ich versuche, mein Buch so informativ und aktuell wie möglich zu halten und dir eine gute Mischung zwischen konkreter Technik und langfristigen Grundsätzen zu vermitteln. Aus Gründen der Lesbarkeit verwende ich die männliche Form, alle anderen Geschlechter, Identitäten und Zugehörigkeiten sind aber selbstverständlich mitgemeint.